CMMC Phase 2 Did Not Start on 10 November 2026: What Still Binds Defense Contractors

HARDAC Industries LLC — Security Advisory HARDAC-ADV-2026-05

Published 14 November 2026 · Version 1.0

Author: HARDAC Industries LLC. Canonical URL: https://hardac.org/advisories/hardac-adv-2026-05/ · Change log: v1.0, initial release.

Summary

The regulation that sets the CMMC phases still reads as written: Phase 2, under which DoD intends to require Level 2 (C3PAO) certification as a condition of award, "Begins one calendar year following the start date of Phase 1." Phase 1 began on 10 November 2025, so the date in the rule text is 10 November 2026. That date has passed without Phase 2. On 13 July 2026 the Department of War (DoW) suspended "the transition to Phase II requirements of CMMC, as well as pending and future CMMC implementation milestones," and opened a 60-day review by a CMMC Reform Task Force. As of this advisory's date, the DoW CIO has published no restart date and no task force report, and 32 CFR 170.3 has not been amended.

What did not pause is everything that applied before Phase 2. DFARS 252.204-7012 still requires NIST SP 800-171 on covered contractor information systems; DFARS 252.204-7019 and 252.204-7020 still require a current assessment score in SPRS; and a contract carrying DFARS 252.204-7021 at Level 1 (Self) or Level 2 (Self) still requires an annual affirmation of continuous compliance by a named affirming official. DoW said it will enforce NIST SP 800-171 "through self-assessments and select government-led assessments," and the Justice Department announced two False Claims Act settlements over NIST SP 800-171 compliance after the suspension, on 1 September and 3 November 2026. Until Phase 2 resumes, the self-assessment score and the affirmation are the record DoW relies on.

This advisory sets out what the suspension changed, what it left in force, and the records a contractor can put in order before a restart, which the task force is reported to have proposed could come over 90 days.

1. What the Rule Text Says, and What Happened Instead

Date	Instrument	What It Says or Does	Source
15 Oct 2024	32 CFR Part 170 (CMMC Program final rule)	Four phases. Phase 1 begins on the effective date of the 48 CFR rule;	[5]

		Phase 2 "Begins one calendar year following the start date of Phase 1"	
10 Sep 2025	DFARS final rule, 90 FR 43560 (DFARS Case 2019-D041)	Adds DFARS 252.204-7021 (NOV 2025) and 252.204-7025; "This rule is effective November 10, 2025"	[6]
10 Nov 2025	Phase 1 begins	Level 1 (Self) or Level 2 (Self) as a condition of award where the requirement is included	[5][6]
13 Jul 2026	DoW press release; CIO memorandum *Removing Barriers to DIB Expansion*; USD(A&S) memorandum 26-P-1023, *Implementing Suspension of CMMC Phase II*	Phase 2 and later milestones suspended; Phase 1 self-assessment requirements "remain firmly in place"; 60-day task force review; RFI to industry	[1][2][3]; (S) [4]
14 Aug 2026	RFI responses due	Industry comments on compliance burden	(S) [14][15]
early Sep 2026	Task force findings to the DoW CIO	Not published by DoW; contents known only from press reporting	(S) [14][15]
10 Nov 2026	Phase 2 date under the rule text	Passed without Phase 2; no restart date announced	[2][5]

32 CFR 170.3 on eCFR, current to 12 November 2026, carries the original phase text unchanged [5]. The rule describes what DoD "intends to include" in each phase; the suspension is a DoW decision about what goes into solicitations and contracts, made by memorandum, not an amendment of the rule.

2. What the Suspension Changed

- **Third-party certification as a new condition of award.** DoW suspended "the transition to Phase II requirements of CMMC, as well as pending and future CMMC implementation milestones across the Department of War solicitations and contracts." [1] As reported by counsel, the implementing memorandum directs that Level 2 (C3PAO) requirements be removed from solicitations (S) [4]. The memorandum itself was not retrievable by automated means for this advisory; the details should be checked against it [3].
- **Later phases.** In our reading, the release's suspension of "pending and future CMMC implementation milestones" covers Phase 3 (Level 2 (C3PAO) for all applicable contracts, Level 3 (DIBCAC) as a condition of award) and Phase 4 (full implementation) [1][5].
- **The program's direction.** The release frames the review as replacing "bureaucratic compliance with scalable, resilient cybersecurity measures" for small, medium and non-traditional businesses [1]. The CIO's "Brilliant at the Basics" campaign, linked from the release, lists ten IT practices for the DIB, led by phishing-resistant multifactor authentication and asset inventory [16].

3. What It Did Not Change

DFARS 252.204-7012. The release: "All defense contractors and subcontractors remain contractually obligated to safeguard covered defense information in accordance with DFARS clause 252.204-7012." [1] The clause (MAY 2024) requires NIST SP 800-171 on covered contractor information systems; incident reports to DoD "within 72 hours of discovery of any cyber incident"; and, for any external cloud service provider holding covered defense information, that the contractor "require and ensure" security "equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline" [7].

DFARS 252.204-7019 and 252.204-7020 (NOV 2023). For award, the offeror "shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation)," with summary scores posted in SPRS [8]. The contractor "shall provide access to its facilities, systems, and personnel" for a Government Medium or High assessment, and shall not award a subcontract subject to NIST SP 800-171 unless the subcontractor "has completed, within the last 3 years, at least a Basic NIST SP 800–171 DoD Assessment" [9]. These are the "select government-led assessments" the release refers to [1].

DFARS 252.204-7021 (NOV 2025), where a contract carries it. The contractor shall "Have and maintain for the duration of the contract a current CMMC status" at the level the contracting officer inserts; process FCI or CUI only on systems with that status; "Complete on an annual basis, and maintain as current, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance" in SPRS for each CMMC UID; ensure subcontractors complete affirmations before subcontract award and annually; and flow the clause down [10]. A Final Level 2 (Self) status is current for three years, with an affirmation "not older than 1 year" [10].

Certificates already issued. None of the instruments cited here withdraws a Final Level 2 (C3PAO) status already issued. Reported counts of companies holding one range from about 2,000 to about 2,500 (S) [14][17].

4. Enforcement After the Suspension

The Justice Department continues to resolve False Claims Act cases built on NIST SP 800-171 obligations that predate Phase 2. Both settlements below were announced after 13 July 2026. In each, the claims "are allegations only and there has been no determination of liability."

- **1 September 2026, Honeywell Aerospace Inc., $2,042,518.** Allegations that from April 2020 through December 2023 a business unit failed to comply with NIST SP 800-171 "with respect to one of Honeywell's networks, as required by the contract and regulation." A whistleblower suit. [12]
- **3 November 2026, ILC Dover LP and ILC Astrospace LLC, $13 million.** Allegations covering January 2018 to October 2024: CUI stored with a cloud provider without ensuring FedRAMP Moderate equivalence; no system security plan for each covered system for long periods; NIST SP 800-171 controls not fully implemented; plans of action and milestones not developed; and, for ILC Astrospace, no current NIST SP 800-171 assessment submitted to DoD from November 2020 to October 2024. [11]

Each allegation in the ILC matter corresponds to a clause in Section 3: the cloud provider to 7012, the system security plan and plans of action to NIST SP 800-171 as 7012 requires it, and the missing assessment to 7019 and 7020. None depends on CMMC Phase 2.

5. What the Task Force Is Reported to Have Proposed

DoW has not published the task force's report. Federal News Network reported on 27 October 2026 that it had obtained a DoD summary of the findings (S) [14]. As reported, and not confirmed by DoW:

- "Over a 90-day period, the task force says DoD could restart Phase 2 of CMMC with a narrower population, while working on longer-term recommendations through the rulemaking process."
- Changes possible without rulemaking: resolving assessor inconsistency, NIST SP 800-171 Revision 3, CUI marking.
- An extension of plan-of-action-and-milestones eligibility to 270 days, which "would require rulemaking."
- Credit for comparable ISO/IEC 27001 requirements; approved configurations and templates; machine-readable (OSCAL) evidence.

Practical reading. If DoW adopts the reported restart model, a contractor in the narrower population could face a Level 2 (C3PAO) requirement about 90 days after an announcement. Assessment capacity was already short before the suspension: the SBA cited "only about 100 approved assessors" for more than 120,000 small businesses [13], and one former official told FNN that most C3PAOs had "dance cards filled through rest of 2026" (S) [14].

6. Questions

Question	Answer
Is CMMC cancelled?	No. Phase 2 and later milestones are suspended pending review. Phase 1 self-assessment requirements "remain firmly in place," and 32 CFR Part 170 is unchanged. [1][5]
Can a solicitation still require Level 2 (C3PAO)?	As reported, the implementing memorandum has Level 2 (C3PAO) requirements removed from solicitations during the suspension. The level that binds is the one the contracting officer inserts in each solicitation's 252.204-7021. (S) [4][10]
My contract already says Level 2 (C3PAO). What now?	The contract text governs until a modification changes it. Ask the contracting officer in writing whether a modification is coming, and keep the answer. [10]
Does our existing Level 2 (C3PAO) certificate still count?	Nothing cited here withdraws it. It satisfies a Level 2 (Self) requirement ("at the following CMMC level, or higher") and still needs the annual affirmation. [10]
Is our SPRS score still required?	Yes, for any award subject to 252.204-7019: current means not more than three years old. [8]
Does the suspension reduce False Claims Act exposure?	Not on the record so far. Both settlements in Section 4 were announced after the suspension and rest on obligations that predate Phase 2. [11][12]
Should we stop preparing for a C3PAO assessment?	That is a business decision. The facts: no restart date; a reported 90-day restart model for a narrower population; limited assessor capacity. A system ready

	for a C3PAO is also the system the SPRS score and affirmation describe. [14][13]

7. Action Steps

1. **Check the SPRS record.** Score date within three years; score matching the current system security plan and open plans of action; one entry for each covered system.
2. **Check the affirmation.** For each contract with 252.204-7021: who the affirming official is, the date of the last affirmation, and whether anything in the system has changed since. The affirmation states continuous compliance, so a change in the system is a reason to review it before the next annual date.
3. **Check cloud providers.** For every external service that stores, processes or transmits covered defense information: written evidence of FedRAMP Moderate authorization or equivalence, and the incident reporting, malware, media preservation and forensic access terms 7012 lists [7].
4. **Collect subcontractor records.** A Basic assessment within three years for each subcontractor subject to NIST SP 800-171 [9]; affirmations before award where 7021 flows down [10].
5. **Read every new solicitation's 7021 fill-in** and every contract modification touching CMMC, and keep the contracting officer's written answers.
6. **Keep the system security plan current.** Every ILC allegation in Section 4 traces to a document that was missing or out of date.
7. **Watch for the restart.** The DoW CIO CMMC page [2], the Federal Register, and the 252.204-7021 text on acquisition.gov [10]. A rulemaking on POA&M terms or Revision 3 would open a comment period.

What This Does Not Cover

The text of the two July 2026 memoranda, which were not retrievable by automated means at publication; the class deviations that implement them; Level 3 (DIBCAC); NIST SP 800-171 Revision 3, which DoD has not adopted into CMMC; the FAR CUI rule; the FIPS validation questions in HARDAC-ADV-2026-01 and the post-quantum deadlines in HARDAC-ADV-2026-04; and any forecast of when or in what form Phase 2 resumes. Statements about the task force's findings come from press reporting of a document DoW has not published.

About HARDAC

HARDAC Industries LLC is a managed security services provider and compliance consultancy, in business ten years, delivering ISO/IEC 27001 and NIST Risk Management Framework consulting and managed security operations to defense contractors and commercial clients. This advisory is general guidance, not legal advice or an assessment finding; contractors should confirm each instrument's current text and their own assessor's and contracting officer's expectations.

Sources

Primary sources are rule text, clauses, agency releases and Justice Department releases; (S) marks secondary. All accessed 14 November 2026 unless noted.

8. Department of War, Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements, press release, 13 July 2026. https://www.war.gov/News/Releases/Release/Article/4542329/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require/
9. DoW CIO, Cybersecurity Maturity Model Certification page, listing the press release and the memoranda *Removing Barriers to DIB Expansion* and *Implementing Suspension of CMMC Phase II*. https://dowcio.war.gov/CMMC/
10. USD(A&S), memorandum 26-P-1023, Implementing Suspension of CMMC Phase II, 13 July 2026. https://dowcio.war.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf ; https://dodcio.defense.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf . Not retrievable by automated means (HTTP 403) at publication.
11. (S) Crowell & Moring, Department of War Immediately Suspends CMMC Phase II Requirements, Launches 60-Day Reform Review, 13 July 2026, updated 14 July 2026. https://www.crowell.com/en/insights/client-alerts/department-of-war-immediately-suspends-cmmc-phase-ii-requirements-launches-60-day-reform-review
12. 32 CFR 170.3(e), CMMC Program, phased implementation; eCFR up to date as of 12 November 2026. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-A/section-170.3
13. DoD, Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), final rule, 90 FR 43560, 10 September 2025, effective 10 November 2025. https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of-cybersecurity-requirements
14. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024). https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
15. DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements (NOV 2023). https://www.acquisition.gov/dfars/252.204-7019-notice-nist-sp-800-171-dod-assessment-requirements.
16. DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements (NOV 2023). https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171-dod-assessment-requirements.
17. DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements (NOV 2025). https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements.
18. Department of Justice, Defense and Aerospace Contractors ILC Dover and ILC Astrospace Agree to Pay $13M to Resolve Cybersecurity Fraud Allegations, 3 November 2026.

https://www.justice.gov/opa/pr/defense-and-aerospace-contractors-ilc-dover-and-ilc-astrospace-agree-pay-13m-resolve
19. Department of Justice, Honeywell Aerospace Inc. Agrees to Pay Over $2M to Settle False Claims Act Allegations of Failing to Comply with Cybersecurity Requirements in a U.S. Department of Defense Contract, 1 September 2026. https://www.justice.gov/opa/pr/honeywell-aerospace-inc-agrees-pay-over-2m-settle-false-claims-act-allegations-failing
20. U.S. Small Business Administration, SBA Commends U.S. Department of War's Suspension of CMMC Phase II for Small Defense Contractors, news release 26-73, 13 July 2026. https://legacy.sba.gov/article/2026/07/13/sba-commends-us-department-wars-suspension-cmmc-phase-ii-small-defense-contractors
21. (S) Federal News Network, RFI offers path forward for DoD with CMMC, 27 October 2026. https://federalnewsnetwork.com/defense-main/2026/10/rfi-offers-path-forward-for-dod-with-cmmc/
22. (S) CMMC Map, The CMMC Task Force Reports in September, published 31 August 2026, updated 16 October 2026 (vendor publication). https://cmmcmap.com/blog/cmmc-task-force-september-report/
23. DoW CIO, Brilliant at the Basics. https://dowcio.war.gov/BrilliantBasics/
24. (S) Federal News Network, Cyber AB's Matthew Travis on CMMC reform, 14 September 2026. https://federalnewsnetwork.com/technology-main/2026/09/cyber-abs-matt-travis-on-cmmc-reform/

Change Log

- 1.0, 14 November 2026: first publication.